UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,930	10/19/2005	Sami Vaarala	290.1078USN	1571

33369 7590 03/23/2010

FASTH LAW OFFICES (ROLF FASTH)
26 PINECREST PLAZA, SUITE 2
SOUTHERN PINES, NC 28387-4301

EXAMINER	
TOWFIGHI, AFSHAWN M	
ART UNIT	**PAPER NUMBER**
2458	

NOTIFICATION DATE	DELIVERY MODE
03/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sloan.smith@fasthlaw.com
nan_russell@fasthlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/500,930	VAARALA ET AL.	
	Examiner	Art Unit	
	AFSHAWN TOWFIGHI	2458	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

2. Claims 1, 22, and 27 are amended.

Response to Arguments

3. Applicant's arguments filed 10/29/2009 have been fully considered but they are not persuasive.

On page 10 of the applicant's response, the applicant argues that Linnakangas teaches negotiating between a remote host and a router, and not negotiating the SA's between the remote host and local host or LAN.

The examiner respectfully disagrees with the applicant's response. Linnakangas teaches that IPSec is used to establish a secure connection between two endpoints (See par. 5, lines 1-6). Linnakangas teaches (See par 4) that IPSec has peer nodes negotiate and exchange keys to establish a secure connection between the two. Each computer does negotiate keys in order to establish a secure connection with other computers on the network. The computer does this via an intermediate computer (router). Once both computers have negotiated a keys using IPSec, then a secure connection between them exists. Inherently, data will be sent to/from each of the computers with each having a respective source/destination address of that secure

connection data path. As the claim language reads, the Linnakangas reference does teach the argued limitations.

On page 14 of the applicant's response, the applicant argues the examiner's interpretation of the IP forwarder as an intermediate computer, and that is simply a component of the router and not an intermediate computer. In addition, the examiner has not found a rationale for the combination within the cited references.

The examiner respectfully disagrees with the applicant's response. As stated above the router acts as an intermediate computer between the secure connection that exists between the two computers. The rationale for the combination of the references comes from a motivation that is obvious to one of ordinary of skill in the art, and does not have to come from the cited references themselves. In this case, the examiner feels that increased security on a network is a motivation to combine one reference with another. Therefore, the cited references do teach the argued limitations.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-5, 7-10, 22-24, 26 & 27 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2001/0047487 to Linnakangas, et al. (Linnakangas).

Regarding claim 1, Linnakangas teaches a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network(See paragraph 24, lines 4-8; wherein the local host 5 is the first computer, remote host 4 is the second computer, and router 2 is the intermediate computer), comprising: the first computer and the second computer negotiating and exchanging keys according to a key exchange protocol to establish a secure connection between the first computer and the second computer via the intermediate computer (See par 4 and "Response to Arguments) (See par. 24, lines 4-11; wherein message formation is inherent in "communication" and "exchanging user generated traffic"), the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection (See par. 8, lines 1-5; wherein the destination of the packets is the second computer) in the first computer, forming a secure message by giving the secure message a first unique identity and a first destination address to the intermediate computer (See par.'s 4 & 24; wherein the SPI is the unique identity, and the header inherently includes the destination address), sending the secure message from the first computer to the intermediate computer (See par. 24, lines 4-6), the intermediate computer receiving the secure message and performing a translation by using the first

unique identity to find a second destination address to the second computer, (See par.'s 4 & 24; wherein a router that is able to perform IPSec and IKE translation, inherently includes a translation table), the intermediate computer substituting the first destination address with the second destination address to the second computer (See par.'s 4 & 24; wherein address substitution is a standard part of IPSec processing and IKE translation), the intermediate computer substituting the first unique identity with a second unique identity of the secure connection without establishing a new secure connection and without involving the second computer, (See par.'s 4 & 24; wherein generating and substituting SPI's is a standard part of IPSec processing and IKE translation; and, par. 8, lines 1-5; wherein a secure association, is the secure connection), and the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection (See par. 24, line 11).

2. Regarding claim 2, Linnakangas discloses forming the secure message in step b) by using an IPSec connection between the first computer and the second computer (See par. 24, lines 4-7).

3. Regarding claim 3, Linnakangas discloses performing a secure forwarding of the message by making use of SSL or TLS protocols (See par. 24, lines 4-7; wherein using a secure socket layer (SSL) is inherent in IPSec).

4. Regarding claim 4, Linnakangas discloses manually performing a preceding distribution of keys to components for forming the IPSec connection (See par. 40, lines

8-12; wherein manual distribution occurs when the IKE module is responding to a request).

5. Regarding claim 5, Linnakangas discloses performing a preceding distribution of keys for forming the IPSec connection by an automated key exchange protocol (See par. 40, lines 8-12; wherein automated key exchange occurs when the IKE module initiates negotiations).

6. Regarding claim 7, Linnakangas teaches sending the message that is sent from the first computer as a packet that contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer (See par. 3, lines 1-6).

7. Regarding claim 8, Linnakangas teaches the IPSec connection being one or more security associations (SA) and the unique identity being one or more SPI values (See par. 4, lines 5-14).

8. Regarding claim 9, Linnakangas teaches performing the matching in step d) by using a translation table stored at the intermediate computer (See par. 31, lines 1-6; wherein the IP forwarder module is part of the intermediate computer).

9. Regarding claim 10, LInnakangas teaches changing both the address and the SPI-value by the intermediate computer (See par. 24; wherein IPSec includes replacing addresses in accordance with the translation tables, and assigning a new SPI value to every received packet).

10. Regarding claim 22, Linnakangas teaches a telecommunication network for secure forwarding of messages, comprising: a first computer, a second computer and

an intermediate computer, means for negotiating and exchanging keys, according to a key exchange protocol, between the first computer and the second computer to establish a security association (See par 4 and "Response to Arguments) (See par. 24, lines 1-15; wherein local host 5 is the first computer, remote host 4 is the second computer, and router 2 is the intermediate computer), having a source address of the first computer as a first end point and a destination address of the second computer as a second end point (See par.'s 5, lines 1-6, and par. 8, lines 1-5), the first and the second computers having means for performing an IPSec processing, the intermediate computer having translation means for using translation tables to perform IPSec and IKE translation (See par. 14, lines 1-5) and for changing a destination address of the intermediate computer of a secure message to a destination address of the second computer, and the intermediate computer having means for forwarding the secure message received from the first computer to the second computer in the secure connection (See par. 8, lines 1-5).

11. Regarding claim 23, Linnakangas teaches the translation table for IPSec translation has IP addresses of the intermediate computer to be matched with IP addresses of the second computer (See par. 24, lines 4-6; wherein the router inherently has translation tables to perform IPSec).

12. Regarding claim 24, Linnakangas teaches the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer (See par. 24, lines 4-8; wherein

the router (or intermediate computer) inherently includes at least two translation tables (or partitions), since one translation table is required for each IPSec connection, and there are at least two IPSec connections).

13. Regarding claim 26, Linnakangas teaches another translation table for IKE translation containing fields for matching a given user to a given second computer (See par. 24, lines 8-11; wherein each remote host must establish a new secure connection, which includes a new translation table).

14. Regarding claim 27, this claim recites a network for carrying out the method of claim 1, and is rejected for the same reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 6, 11-14 & 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnakangas, as applied to claim 1 above, in view of Applicant's Admitted Prior Art (AAPA).

16. Regarding claim 6, Linnakangas teaches the invention as described in claim 5. Linnakangas does not teach performing the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection by means of a

modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer. However, AAPA teaches a modified IKE key exchange protocol between the first computer and the intermediate computer (See page 8, lines 27-29; wherein the key exchange is modified to support NAT traversal) and a standard IKE key exchange protocol between the intermediate computer and the second computer (See p. 8, lines 29-32).

Using the features of AAPA in the system of Linnakangas would have added flexibility by allowing different networks to connect to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

17. Regarding claim 11, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach the first computer being a mobile terminal, so that the mobility is enabled by modifying the translation table at the intermediate computer. However, AAPA teaches this limitation (See p. 7, lines 10-16).

Using the features of AAPA in the system of Linnakangas would have broadened the appeal and applicability of the system by allowing mobile units to connect to the network. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

18. Regarding claim 12, Linnakangas, in view of AAPA, teach the invention as described in claim 11. Linnakangas further teaches performing the modification of the

translation tables by sending a request for registration of the new address from the first computer to the intermediate computer (See p. 3, par.'s 46-51).

19. Regarding claim 13, Linnakangas, in view of AAPA, teach the invention as described in claim 12. Linnakangas further teaches sending a reply to the request for registration from the intermediate computer to the first computer (See p. 3, par. 50).

20. Regarding claim 14, Linnakangas, in view of AAPA, teach the invention as described in claim 12. Linnakangas further teaches authenticating or encrypting by IPSec the request for registration and/or reply (See p. 3, par. 62).

21. Regarding claim 20, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach sending the secure message by using an IPSec transport mode. However, AAPA teaches this limitation (See p. 4, lines 14-19).

Using the features of AAPA in the system of Linnakangas would have added improved security to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

22. Regarding claim 21, Linnakangas teaches the invention as described in claim 1. Linnakangas does not teach sending the secure message by using an IPSec tunnel mode. However, AAPA teaches this limitation (See p. 4, lines 21-29).

Using the features of AAPA in the system of Linnakangas would have added improved security and flexibility to the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of AAPA and Linnakangas.

23. Claims 15-19 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnakangas, as applied to claims 4 & 24 above, in view of U.S. Patent Number 6,985,953 issued to Sandhu, et al. (Sandhu).

24. Regarding claim 15, Linnakangas teaches the invention as described in claim 4. Linnakangas further teaches establishing the key distribution for the secure connections by establishing an IKE protocol translation table, and using the translation table to modify IP addresses of IKE packets in the intermediate computer (See par. 24, lines 4-6). Linnakangas does not teach using the translation table to modify cookie values of IKE packets in the intermediate computer. However, Sandhu teaches this limitation (See col. 7, line 55 to col. 8, line 19; wherein the KDC is the intermediate computer).

Using the features of Sandhu in the system of Linnakangas would have added another layer of security within the secure connection. Therefore, it would have been obvious to one of ordinary skill, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

25. Regarding claim 16, Linnakangas in view of Sandhu teach the invention as described in claim 15. Linnakangas does not teach establishing the key exchange distribution by: generating an initiator cookie and sending a zero responder cookie to the second computer, generating a responder cookie in the second computer, and establishing a mapping between IKE cookie values in the intermediate computer. However, Sandhu teaches generating an initiator cookie and sending a zero responder cookie to the second computer (See col. 8, lines 41-47; wherein the Authenticator is the

initiator cookie), generating a responder cookie in the second computer (See col. 8, lines 41-47; wherein Bob's response is the responder cookie), and establishing a mapping between IKE cookie values in the intermediate computer (See col. 8, lines 49-51; wherein a mapping is required for authentication).

Using the features of Sandhu in the system of Linnakangas would have increased the number of security features available in the system. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

26. Regarding claim 17, Linnakangas in view of Sandhu teach the invention as is described in claim 15. Linnakangas further teaches modifying a IKE protocol between the first computer and the intermediate computer by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modify IKE packets (See par.'s 4 & 24; wherein the remote host 4 is an IPSec node that sends the IKE keys, and equates to applicant's first computer).

27. Regarding claim 18, Linnakangas in view of Sandhu teach the invention as is described in claim 15. Linnakangas further teaches carrying out the modification of the IKE packets by the first computer with the intermediate computer requesting such modifications (See par.'s 41-45; wherein the IKE module is in the intermediate computer).

28. Regarding claim 19, Linnakangas in view of Sandhu teach the invention as described in claim 17. Linnakangas further teaches defining the address so that the first computer is identified for the second computer by the intermediate computer by means

of an IP address taken from a pool of user IP addresses when forming the translation table (See par.'s 56 & 57).

29. Regarding claim 25, Linnakangas teaches the invention as described in claim 24. Linnakangas further teaches both partitions of the mapping table for IKE translation contains translation fields for a source IP address and a destination IP address between respective computers (See par. 24, lines 4-8; wherein source and destination addresses are inherent in IPSec). Linnakangas does not teach the mapping table for IKE translation contains translation fields for initiator and responder cookies between respective computers. However, Sandhu teaches a mapping table that contains translation fields for initiator and responder cookies between respective computers (See col. 8, lines 41-51; wherein the authenticator is the initiator cookie and Bob's response is the responder cookie).

Using the features of Sandhu in the system of Linnakangas would have provided increased security and insured that messages where transmitted to the correct destination. Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention, to combine the teachings of Sandhu and Linnakangas.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AFSHAWN TOWFIGHI whose telephone number is (571)270-7296. The examiner can normally be reached on Monday - Friday 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph E. Avellino can be reached on (571)272-3905. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. T./
Examiner, Art Unit 2458

/Joseph E. Avellino/
Supervisory Patent Examiner, Art Unit 2458